REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
10-06-2016	Master's Thesis	27-07-2015 to 10-06-2016

4. TITLE AND SUBTITLE

U.S. MILITARY TECHNOLOGY DEPENDENCE: THE HIDDEN VULNERABILITY TO NATIONAL SECURITY

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lt Col. Keven P. Coyle, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

National Defense University
Joint Forces Staff College
Joint Advanced Warfighting School
7800 Hampton Blvd
Norfolk, VA. 23511-1702

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release, distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Because the U.S. has a technological culture, the U.S. military has become technology dependent. This dependence has made the military more vulnerable and has plunged the DoD into a perpetual cycle of purchasing technology to fill shortfalls resulting from reductions in manpower, technology evolutions, and to "maintain the leading edge." Because technology is increasing in per-unit cost, the DoD purchases fewer items which increases the impact of minimal losses in combat. It is feasible that while technology can make warfighting more efficient, the military can become so technology dependent that the organization no longer recognizes that technology has made it more vulnerable strategically, operationally, and tactically. The United States military is going through a cyclic downsizing of force strength; when all the people are gone, where does the military turn to backfill human capacity? This thesis will address three fallacies associated with overdependence on technology in the U.S. military: first, that technology reduces manpower requirements, second that it is less expensive to use technology in lieu of humans in warfighting, and finally, that incorporating technology in operations ensures a decisive victory in today and future conflicts. Reversing technology dependence requires better integration, complementary technologies among the services, decreasing the innovation to fielding timeline, and practice in degraded technology environments.

15. SUBJECT TERMS
Vulnerability, Culture, Military, Sociology, Threat, Technology, Technological

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Director of JAWS
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED/ UNLIMITED	66	19b. TELEPHONE NUMBER *(include area code)* 757-443-6301

NATIONAL DEFENSE UNIVERSITY

JOINT FORCES STAFF COLLEGE

JOINT ADVANCED WARFIGHTING SCHOOL

U.S. MILITARY TECHNOLOGY DEPENDENCE: THE HIDDEN VULNERABILITY TO NATIONAL SECURITY

by
Keven P. Coyle
Lieutenant Colonel, United States Air Force

Intentionally left blank

U.S. MILITARY TECHNOLOGY DEPENDENCE: THE HIDDEN VULNERABILITY TO NATIONAL SECURITY

by Keven P. Coyle
Lieutenant Colonel, United States Air Force

A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy. The contents of this thesis reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

This thesis is entirely my own work except as documented in footnotes.

Signature: _____

10 June 2016

Thesis Advisor: Signature: _____

Dr. S. M. Pavelec, Thesis Advisor

Approved by: Signature: _____

Kevin Therrien, Col, USAF
Committee Member

Signature: _____

Peter E. Yeager, Col, USMC
Director, Joint Advanced Warfighting School

Intentionally left blank

ABSTRACT

Because the U.S. has a technological culture, the U.S. military has become technology dependent. This dependence has made the military more vulnerable and has plunged the DoD into a perpetual cycle of purchasing technology to fill shortfalls resulting from reductions in manpower, technology evolutions, and to "maintain the leading edge." Because technology is increasing in per-unit cost, the DoD purchases fewer items which increases the impact of minimal losses in combat. It is feasible that while technology can make warfighting more efficient, the military can become so technology dependent that the organization no longer recognizes that technology has made it more vulnerable strategically, operationally, and tactically.

The United States military is going through a cyclic downsizing of force strength; when all the people are gone, where does the military turn to backfill human capacity? This thesis will address three fallacies associated with overdependence on technology in the U.S. military: first, that technology reduces manpower requirements, second, that it is less expensive to use technology in lieu of humans in warfighting, and finally, that incorporating technology in operations ensures a decisive victory in today and future conflicts. Reversing technology dependence requires better integration, complementary technologies among the services, decreasing the innovation to fielding timeline, and practice in degraded technology environments.

Intentionally left blank

DEDICATION

This thesis is dedicated to my sweet wife who has gracefully led our family through thick and thin throughout the years and especially during the countless hours of research, travel, and study associated with the writing of this thesis. Additionally, I dedicate this thesis to my children who have sacrificed birthdays, holidays, and precious time as I have pursued a career in the United States military and who will inherit the world we leave them, good and bad.

Intentionally left blank

ACKNOWLEDGEMENTS

I would like to offer special thanks to my advisors Dr. Mike Pavelec and Colonel Kevin Therrien without whose advice, patience, challenge, and direction the ideas presented in this thesis would not have been developed. I would also like to thank Mr. Jeffrey Turner from the Joint Force Staff College (JFSC) Writing Center, and the great staff of the JFSC Library for facilitating the availability of resources from all over the region so I could conduct the detailed research required for this culmination of this thesis.

Intentionally left blank

TABLE OF CONTENTS

INTRODUCTION 1
Issue 1
Research Approach 2
Research Limitations 2
Synthesizing Definitions 3
TECHNOLOGICAL CULTURE 9
Military Strategy in Technological Culture 10
Vulnerability Assessment in Technological Culture 12
Technological Culture Model Overview 14
THE MODEL 18
SECTION 1: Requirements Generation 18
Presumptive Anomaly 18
Military Derived Requirements 19
Industry Driven Requirements 20
SECTION 2: Technology Development 22
Budgetary Considerations and Strategic Direction 23
Military Research and Development 24
Industry Research and Design 25
Bridging the Technology Gap between DoD and Industry 26
SECTION 3: Acquisition of New Technology 27
Acquisition Process Overview 27
Understanding Intrinsic Vulnerability 28
Identifying Internal / External Vulnerabilities 29
SECTION 4: Fielding New Technology 32
Understanding the Complexity of the System 33
Integration Considerations 34
Interoperability Considerations 36
SECTION 5: The Role of Disruptive Technology 37
Revolutions in Military Affairs 37
Technological Advances in Warfare 37
CHAPTER 3: BREAKING THE CYCLE 39
Seeking Joint Solutions 39
Reducing the Idea-to-Fielding Timeline 40
CONCLUSION 42
APPENDIX 1 47
APPENDIX 2 48
APPENDIX 3 49
BIBLIOGRAPHY 50
VITA 55

Intentionally left blank

INTRODUCTION

Issue

The United States has a technological culture. By extension, the United States military has become technology dependent, and thereby more vulnerable. There are numerous authors who have written on the topic of technology, or more specifically on technological culture[1] and the sociology of the military.[2] What is missing in the literature is the specific application of a technological culture model illustrating the development of military technology dependence and vulnerability. It is feasible that while technology can make warfighting more efficient, the military can become so technology dependent that the organization no longer recognizes that technology has made it more vulnerable strategically, operationally, and tactically.

In America today, technology infuses everything from dishwashers to drones, picture frames to phones, and bullets to bones.[3] It seems that any inefficiency can be resolved by adding a sprinkle of technology pixie dust. It is not uncommon in the 21st Century to hear, "well, email is down, I guess we can all go home for the day," or "is there an app for that?" The United States military is going through a cyclic downsizing of force strength; when all the people are gone, where does the military turn to backfill human capacity? In this century, it has turned to robots, distributed mission operations (DMO), and virtual training. This thesis will address three fallacies associated with overdependence on technology in the U.S. military: first, that technology reduces

---

[1] Alastair Finlan. *Contemporary Military Culture and Strategic Studies: US and UK armed forces in the 21st Century*. (Routledge, 2013).
[2] Giuseppe Caforio. *Handbook of the Sociology of the Military*. (Springer Science & Business Media, 2006).
[3] Michio Kaku. *Physics of the Future: How Science Will Shape Human Destiny and our Daily Lives by the Year 2100*. (Anchor, 2012). Multiple pages.

manpower requirements, second, that it is less expensive to use technology in lieu of humans in warfighting, and finally, that incorporating technology in operations ensures a decisive victory in today and future conflicts.

To frame the concept, the thesis will describe and define a new "Technological Culture Model" (Appendix 1). The model depicts how the existing paradigm of seeking technology to solve issues in a highly complex and interdependent system perpetuates technology dependence and increases intrinsic, internal and external vulnerabilities into the system. Historical examples and current research inform the model to demonstrate how the United States military has become technology dependent and articulate why it is detrimental to national security.

Research Approach

This thesis will review existing Department of Defense (DoD) documents, books, articles, interviews and historical material to investigate vulnerabilities that have been accepted by the integration and employment of evolving technology in the United States military. The thesis will present analytical arguments through examples of when technological change has reshaped the character of war and where current program efforts have failed to make the United States military more effective in fighting on the battlefields of the 21st Century.

Research Limitations

This argument does not account for all of the vulnerabilities that already exist in a complex system but addresses where technology has driven military dependence and created exploitable vulnerabilities. It will highlight areas where vulnerability exists that has been recognized, accepted, and allowed but not accounted for as the complex system

changes with evolving technology. The focus of this thesis is military operations and functions. All discussions and references are from unclassified sources. Research included Official Use Only documents; however, this thesis only references unrestricted information.

Synthesizing Definitions

In researching technological culture, definitions can sometimes be difficult to come by, or at least difficult to pin down, as each scholar defines terms differently. Baselining terms like disruptive technology, interoperability, presumptive anomaly, risk, vulnerability and complexity are informative to technological culture and to the development of technology dependence. Dr. Thomas Mahnken asserts that technology has had an important influence on the American way of war and is a defining factor in shaping service cultures in the military. He further describes cases where the strategy of the United States has interacted with technology in surprising and often unexpected ways.[4]

Disruptive Technology

Callaway and Hamilton introduce the idea of "disruptive technology", or technology that, when introduced to an environment, fundamentally changes the environment or established paradigm.[5] Examples of disruptive technology include gunpowder, the invention of heavier than air flight, nuclear weapons, and directed energy

[4] Thomas G. Mahnken. *Technology and the American Way of War*. (Columbia University Press, 2008) 22.
[5] S. K. Callaway and R. D. Hamilton, "Exploring Disruptive Technology: The Structure and Control of Internal Corporate Ventures." *International Journal of Organizational Analysis, 14*(2), (December 2006) 87-106. Retrieved from http://search.proquest.com.nduezproxy.idm.oclc.org/docview/198743036?accountid=12686 (accessed November 22, 2015)

weapons.[6] It should be noted that disruptive technology has been referred to in other ways. Ian Morris calls disruptive technology, "Revolutions in Military Affairs" (RMA), meaning the very existence of these technological advances plus the changes in thinking results in a change in the character of warfare.[7] For the sake of this thesis, consider the physical properties of an RMA and disruptive technology to be synonymous.

Interoperability

Interoperability is "The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces, and to use the services so exchanged to enable them to operate effectively together."[8] Interoperability does not only mean the ability for various technologies to share information or work together seamlessly, it also has a coalition nature to it. Joint Vision 2020 directs that, "Interoperability is a mandate for the joint force of 2020, especially in terms of communications, common logistics items, and information sharing. Information systems and equipment that enable a common relevant operational picture must work from shared networks that can be accessed by any appropriately cleared participant."[9] When it comes to complexity, interoperability is, "the successful adaptation of complex systems…requiring some level of cooperation among the agents within the system."[10]

---

[6] Andrew Oram. *Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology*. (*O'Reilly Media, Inc.*, February 26, 2001)
[7] Ian Morris. *War! What is it Good For?: Conflict and the Progress of Civilization from Primates to Robots*. (Macmillan, 2014) 386.
[8] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Pub 1-02 (Washington DC: Joint Chiefs of Staff, November 8, 2010), 118.
[9] U.S. Joint Chiefs of Staff, *Joint Vision 2020*, (Washington DC. Joint Chiefs of Staff, Summer 2000), 9.
[10] Norman N. Axelrod, "Embracing Technology: The Application of Complexity Theory to Business." *Strategy & Leadership*, no. 6 (October 1999), 56-8, http://search.proquest.com.nduezproxy.idm.oclc.org/docview/194363285?accountid=12686. (accessed October 5, 2015)

Presumptive Anomaly

Dr. Edward Constant defines a presumptive anomaly by describing that "there exists throughout the military complex system, requirements that are presumed to exist because they will make the whole system better."[11] The anomaly "would seem to represent one direct causal link between theoretical science and technological practice," meaning that a presumptive anomaly is a technology that is presumed to be developed based on a known future requirement.[12] Presumptive anomalies influence the Technological Culture Model by establishing requirements that are presumed to exist because of service life, evolutions in technological development, or a need to refresh outdated equipment.

Risk vs. Vulnerability

Recognizing the differences and interplay between vulnerability and risk is important in building a foundational understanding of technology analysis and employment decision making in a technological culture. Strategic risk has "the potential to impact the United States – to include our population, territory, and interests – of current and contingency events given their estimated consequences and probabilities"[13] Risk is also "being exposed to the chance of failure"[14] or "the probability of an adverse event of some magnitude, a danger of some kind that can be managed."[15]

---

[11] Edward W. Constant, *The Origins of the Turbojet Revolution*. No. 5. (Johns Hopkins University Press, 1980), 62.
[12] Ibid. 65
[13] Briefing on CJCS Risk Analysis System (August 2, 2004), https://dde.carlisle.army.mil/LLL/DSC/ppt/L14_CRA.pdf, (accessed October 8, 2015)
[14] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Pub 1-02 (Washington DC: Joint Chiefs of Staff, November 8, 2010), 206.
[15] Cynthia Hardy and Steve McGuire, "Organizing Risk, Discourse, Power, and 'Riskification'" *Academy of Management Review* 41., no. 1 (January 2016), 80-108, EBSCO*host,* (accessed 21 January 2016)

"Vulnerability comes from the Latin word vulnus, meaning 'wound.' Vulnerability is the state of being open to injury, or appearing as if you are."[16] Based on the above definitions, a vulnerability is a weakness that is exploitable by an adversary. Risk is the exposure of that weakness to the adversary. Determining the capability of the adversary to capitalize on vulnerabilities and setting appropriate risk levels for military activities is important when conducting strategic, operational, and tactical planning.

Complexity Theory

Complexity theorists also argue over definitions. A system is complex if it consists of an environment where systems are dependent on each other, such that a change to one can result in a cascade of changes in others. The military is a complex system, or a system comprised of many inter-related systems. At the root of complexity theory is the idea that introducing change to the environment can have long-lasting and often initially unperceived effects. Some may argue that systems operate independently, however consensus today is that the systems environment as a whole is one of interdependence.[17] These interdependent systems can be either open or closed systems.

A closed system is one in which all the agents are bound by their own set of rules or parameters, and share a core commonality. In the military, air forces, ground forces, surface forces, information forces, and international forces work together to achieve a myriad of political and military ends. Because each sub-system is reliant upon the other sub-systems to reach desired ends, warfighting becomes a complex system of systems. Each organization has its own set of unique technologies and integrated tactics. Not all

[16] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms,* Joint Pub 1-02 (Washington DC: Joint Chiefs of Staff, November 8, 2010), 256.
[17] S. E. Wallis, "The Complexity of Complexity Theory: An Innovative Analysis." *Emergence: Complexity and Organization,* 11(4), (April 2009), 26-38. http://search.proquest.com.nduezproxy.idm.oclc.org/docview/214151202?accountid=12686 (accessed December 15, 2015)

systems and technologies are interoperable, meaning they do not seamlessly operate together; however, they do interact inside the bounds of the complex system.

A lack of interoperability increases the level of complexity in the system as the soldiers, sailors, marines, or airmen make adjustments, sometimes real-time, in order to integrate non-interoperable systems in the battlespace environment. When a system gets so complex that any change to the system causes secondary catastrophic effects, the system can descend into chaos.[18] "Understanding the mechanisms and structures that drive the dynamic improvements we observe in physical systems can often be useful…" in determining how "agents" or technologies will interact with the system. [19] When the introduction of new technologies affects the system, oftentimes the results are "emergent properties." Emergent properties define requirements and are adaptations made in the system allowing for the integration of new technology. These emergent properties can drive new requirements and are part of the requirement generation process in the Technological Culture Model.

Understanding how a technological culture feeds a technology dependence is imperative. The experiences that influence a non-technical culture to become a technological culture are informative to the establishment of technology dependence in society and in the military. Technology influences almost everything today. The inculcation of that technology into daily life occurs over generations. The technological

[18] J. Snell, "Chaos Theory and Post Modernism." *Education*, 130(2), (February 2009), 274-276. http://search.proquest.com.nduezproxy.idm.oclc.org/docview/196414440?accountid=12686 (accessed 27 September 2015)
[19] Norman N. Axelrod, "Embracing Technology: The Application of Complexity Theory to Business." *Strategy & Leadership*, no. 6 (October 1999), 56-8, http://search.proquest.com.nduezproxy.idm.oclc.org/docview/194363285?accountid=12686. (accessed October 5, 2015)

generation gap is easy to identify, just ask someone born in the 1920’s or 30’s how to find something on the internet.

CHAPTER 1:

TECHNOLOGICAL CULTURE

Culture is "the process whereby tradition is reconfigured in the historical conditions of everyday life and everyday change."[1] Slack frames a culture as a "whole way of life," meaning that the particular shape of a culture is manifested by the process at a particular point in time.[2] To claim "culture is ordinary" is to acknowledge that these cultural processes occur within the variety of practices that constitute everyday life.[3] If culture is a whole way of life, then technology is already a part of everyday life: it exists in the cars we drive, the pens we write with, and the oven in which we cook our food. Technology is not something separable from everyday life and it is not separable from culture.[4]

A technological culture does not evolve overnight. The United States has been developing a culture of technology for centuries. Technology can make processes more efficient and less costly. In the 18th Century, Eli Whitney patented the cotton gin, making cotton harvesting more efficient and profitable, and revolutionized manufacturing with the development of interchangeable parts.[5] In the 19th Century, Henry Ford created the assembly line to streamline vehicle production.[6] Contemplate whether or not the current households of America would be willing to revert back to fireplaces as the sole

---

[1] Jennifer Daryl Slack and J. Macgregor Wise. "Culture and Technology." *A Primer, New*. (August 2005), 25.
[2] Ibid., 36.
[3] Ibid., 58.
[4] Macgregor J. Wise, "Technological Culture: A Presentation to the Asia Cultural Forum 2006." Transcript of presentation given at Kwangju City South Korea June 2006. http://www.cct.gov.kr/data/acf2006/mobile/mobile_keynote2_Macgregor.pdf. (accessed August 15, 2015)
[5] Robert S. Woodbury, "The Legend of Eli Whitney and Interchangeable Parts," *Technology and Culture* 1.3 (1960), 235–253.
[6] Samuel S. Marquis, *Henry Ford: An Interpretation*. (Wayne State University Press, 1923), 12.

source of heating, candles for light, or forego electricity. Technology is inseparably woven into American culture.[7] A technological culture adapts and incorporates technology in such a way that retrograding is very difficult. The U.S. military is a melting pot of cultures including the technological cultures introduced by each individual military member. This is a strength but can also be a weakness. Because the majority of members of the U.S. military are raised in the technological culture of the U.S., they bring varying levels of technology dependence to the military.

Military Strategy in Technological Culture

Strategic culture is not as easy to define; applying strategy to technology is even more daunting. According to Johnston, a strategic culture consists of "predominant strategic preferences that are rooted in the early or formative experiences of the state, and are influenced to some degree by the philosophical, political, cultural, and cognitive characteristics of the state and its elites."[8] Strategic culture is also defined as, "an amalgam of a country's set of shared beliefs, assumptions, and narratives that shape its strategic decision-making process."[9] The United States does not have a stated strategy or direction for technological development despite the National Security Strategy (NSS) stating, "We continue to set the pace for science, technology, and innovation in the global economy."[10] In the National Military Strategy (NMS) 2015, the Chairman of the Joint Chiefs of Staff (CJCS) states, "The United States is the world's strongest nation, enjoying unique *advantages in technology*, energy, alliances, partnerships, and demographics.

[7] Loren Lutzenhiser, "Social Structure, Culture, and Technology: Modeling the Driving Forces of Household Energy Consumption." *Research directions* (1997), 129.
[8] Alastair Iain Johnston, "Thinking About Strategic Culture." *International security* (1995), 32-64.
[9] Jennifer Knepper, "Nuclear Weapons and Iranian Strategic Culture." *Comparative Strategy* 27.5 (2008), 451-468.
[10] U.S. President, *National Security Strategy* (Washington DC: Government Printing Office, February 2015). 2

However, these advantages are being challenged…emerging technologies are impacting the calculus of deterrence and conflict management by increasing uncertainty and compressing decision space."[11] However, the NSS offers no solution to this stated problem.

Evidence of a technological culture in the United States is reflected in the governing strategic documents of today. Numerous strategy documents also cite "technological advantage" as an objective. Although not explicitly stated, accepting that technology is *an* answer, and in some cases *the* answer, technological culture is driving technology dependence in the military. Many would question whether the United States will enter into any conflict without the use of drones, 5th generation fighters, stealth bombers, or computers. U.S. technological advantage is astounding. However, that advantage is tenuous as extremists and non-state actors challenge U.S. resolve to fight as the cost-benefit analysis tips the scales where the cost of employing technology may outweigh the results.[12] Technology is expensive and when adversaries do not have the capital to spend, they turn to inexpensive and innovative ways to gain the asymmetric advantage. For example, terrorists could use a $3 sticker to defeat million dollar precision targeting efforts.[13]

---

[11] Martin Dempsey, *The National Military Strategy of the United States of America, 2015: The United States Military Contribution to National Security*. Joint Chiefs of Staff, (Washington DC: Government Printing Office, 2015).
[12] Conor Freidersdorf, "Obama Supporters Know His Drone War is Indefensible" *The Atlantic: Politics*, (June 7, 2012) http://www.theatlantic.com/politics/archive/2012/06/obama-supporters-know-his-drone-war-is-indefensible/258218/ (accessed January 15, 2016)
[13] Adam Clark Estes, "Your Phone's Battery Use Lets Spies Track Your Movements", *Gizmodo*, (20 Feb 2015), http://gizmodo.com/spies-can-track-you-through-your-phones-battery-use-eve-1686978418, (accessed January 20, 2016).

Vulnerability Assessment in Technological Culture

Some would argue that technology increases efficiency, increases effectiveness, and decreases vulnerabilities.[14] The introduction of technology into a complex system can create more problems than it solves. Vulnerability is defined in three environments: intrinsic,[15] internal,[16] and external vulnerabilities.[17] The definition of risk in Joint Pub 5.0 and the arguments presented by Bijker on vulnerabilities in technological cultures reinforce the notion that the U.S. has a technological culture and thereby is vulnerable to technology dependence.[18] Dr. Jack Douglas' research illustrates that the proliferation of technology has generated a reliance that threatens the American way of life.[19] Douglas argues that the widespread use of technology has an effect on American values, politics, and society as a whole.

Consider the use of remotely piloted aircraft to attack targets in locations thousands of miles from where the operators sit. The initial use of unmanned aircraft spawned heated debates over the ethics of their use in war; however, today drones are no longer for military use only. Recently enthusiasts flying drones all over the U.S. has forced the Federal Aviation Administration (FAA) to institute policies concerning drone operations in proximity to busy airspaces. Drone technology has become smaller and less expensive and drone uses have expanded to include farmers surveying their fields and sports enthusiasts recording their own athletic adventures.

---

[14] Clive Thompson, *Smarter Than You Think: How Technology is Changing our Minds for the Better*. (Penguin, 2013).
[15] Robert Francescotti, "How to Define Intrinsic Properties." *Noûs* (1999): 590-609.
[16] Jennifer Knepper, "Nuclear Weapons and Iranian Strategic Culture." *Comparative Strategy* 27.5 (2008), 451-468.
[17] Norman Loayza and Claudio E. Raddatz. "The Structural Determinants of External Vulnerability." *World Bank Policy Research Working Paper* 4089 (2006). 12
[18] Wieve Eco Bijker, *Vulnerability in Technological Cultures*. (Maastricht University, 2009), 68.
[19] Douglas, Jack D. *The Technological Threat*. (Prentice-Hall, 1971), 32.

Using unmanned machines in war causes an ethical dilemma in warfighting that is still under scrutiny. Some have associated the surgical strike capability of drones to assassination. Over the past 15 years of drone warfare, ethical challenges have begun to slowly redefine traditional American values concerning the employment of robots in war. Keeping an American Airman from harm's way in Nevada while killing an adversary combatant on the other side of the planet is now seen as acceptable. Despite Douglas' 1971 statement, "there is still time to prevent the rise of this technical tyranny," it could be argued that the U.S. has become even more technology reliant than even Douglas foresaw.[20]

While using drones may appear to reduce vulnerability to U.S. service members, it actually increases the vulnerability of the warfighting system. If a drone loses its satellite link, communication with its handler, or has a mechanical malfunction, the loss of the asset can have tactical, operational, and strategic ramifications. The loss of the RQ-170 drone in Iran in December 2011 will likely have significant military, scientific, and political impact for years to come.[21] Additionally, vulnerabilities are introduced into the complex system as well. For example, reducing satellite bandwidth to manned assets in order to facilitate the up-link and down-link frequencies of unmanned systems makes the manned assets more vulnerable to communication exploitation. Aircraft are given limited radio spectrum usage, usually resorting to using ultra-high-frequency (UHF) radios instead of secure beyond line-of-sight (BLOS) satellite radios. The integration of

[20] Ibid., 4.
[21] Dave Majumdar, "Did Iran Just Create Stealth Drone Captured American Tech?" *The National Interest* (November 24, 2014), http://nationalinterest.org/feature/did-iran-just-create-stealth-drone-captured-american-tech-11683 (accessed December 15, 2015)

slower moving, less maneuverable, and hard to see drones into the airspace also increases the collision risk to manned aircraft flying in proximity to unmanned aircraft.

There are significant technical requirements to fly, exploit, and disseminate the data coming from the drone's sensors and these channels are now vulnerable to enemy exploitation, influence, and attack. So while the lives of one or two servicemen in Nevada are no longer at risk in the warfighting environment, the lives of others, the exploitation of information, and the vulnerability of the complex warfighting system has logically increased.

Technological Culture Model Overview

Models are helpful in taking complex concepts and simplifying them to facilitate understanding. Models can also help illustrate a difficult conceptual problem. Visualize the perpetual nature of current military technological culture. Every model must have a starting place; for the Technological Culture Model the starting place is in requirements identification. Requirements generation can drive innovation. The model then walks the reader through technology development, technology procurement, and finally fielding new technologies.

When the military fields new technology, it oftentimes does not integrate seamlessly into the system without requiring adjustments. The introduction of new technology often generates new requirements, especially if the technology is not fully integrated or interoperable within the system. Because of interoperability difficulties, it is not uncommon for systems to adjust while incorporating newer technology in order to gain a technological advantage or to meet some tactical or operational end.

The four main sections of the Perpetual Technology Model are first, an observed need, requirement, or presumptive anomaly that begins the cycle. Second, innovation leading to technology research and development through the United States military laboratories or through the military or private industrial complex leads to technology development. Third, once the technology is designed and developed, it must be budgeted, purchased, leased, or contracted. Fourth, after the technology is acquired, it must be tested and evaluated to determine how, when, and where it will be fielded. Once fielded, leaders, planners and tacticians determine the optimum operational integration strategy and weave the new technology amongst multiple other technologies attempting to achieve interoperability. When the military fields new technology, it disrupts the complex operational environment and oftentimes generates new requirements to allow the incorporation of the newly fielded technology into the operational schema.

Many of the technological disruptions in the operational or tactical environment are the result of vulnerability mitigation efforts inherent to the integration of new technology and the stress induced on the complex system of the battlefield. Mitigating the induced vulnerabilities generates further adjustments or new requirements and the perpetual cycle re-starts.

Sometimes a "presumptive anomaly" drives a new requirement. [22] Other times, disruptive technology will interrupt the cycle driving hasty requirements and rapid innovation. Ultimately, the Technological Culture Model provides a framework for visualizing how the DoD functions in a perpetual technology cycle based on the U.S. technological culture.

[22] Edward W. Constant, *The Origins of the Turbojet Revolution*. No. 5. (Johns Hopkins University Press, 1980), 62.

The model does not illustrate the fact that there are intrinsic, internal, and external vulnerabilities within every new technology and once introduced into a system compounding vulnerabilities can emerge. While technology may temporarily fill gaps in capability, relying too heavily on technology will increase the overall vulnerability of the system.

In an environment of diminishing fiscal resources, it is imperative that the Chairman of the Joint Chiefs of Staff (CJCS) and the Secretary of Defense (SECDEF) recognize that the United States military is caught in a perpetual technology cycle creating greater vulnerabilities at the strategic level, while solving technology challenges at the tactical level. The dependency on technology that is being generated in today's military carries strategic risk. In the 21st century warfighting environment, satellite communication (SATCOM) radios or internet telephones shrink the connection between the tactical level of war and the strategic level. Because the operational gap that used to separate the two environments has shrunk, tactical actions can have strategic impact. For example, the loss of one F-22 fighter aircraft will diminish the total fleet by .55% whereas the loss of a single F-16 aircraft only diminishes the fleet by .001%. Some would argue that this difference in force strength is because one F-22 has the technical capacity and total cost of up to eight F-16s. If that were true, reversing that logic would mean that losing one F-22 will have 8-times the impact of losing one F-16. Because the DoD has to work within the constraints of the budget, and because technology is very expensive, keeping the fleet on the leading edge creates greater vulnerability to the system as a whole because the smaller fleet cannot absorb the potential loss of aircraft nor the loss of capabilities that one aircraft brings to the fight.

CHAPTER 2:

THE MODEL

SECTION 1: Requirements Generation

Requirements come from the military, the military-industrial complex, or because of presumptive anomalies. Throughout the military's complex procurement system, requirements are generated to improve the system or to fill perceived gaps making the whole system function better.[1] This chapter will illustrate three types of requirement generators; presumptive anomalies, military derived requirements and industry driven requirements.

Presumptive Anomaly

Dr. Edward W. Constant III in 1982 coined the term "Presumptive Anomaly" describing the phenomena "when assumptions derived from science indicate either that under some future conditions the conventional system will fail (or function badly) or that a radically different system will do a much better job. No functional failure exists; an anomaly is presumed to exist; hence a presumptive anomaly."[2] Consider this concept in terms of generations of fighter capabilities. Fifth-generation fighters are more capable, are more technical, and are more efficient at fighting than fourth-generation fighters; therefore, it is presumed that the U.S. needs a fifth-generation fighter, subsequently generating a requirement to produce one. The anomaly "would seem to represent one direct causal link between theoretical science and technological practice."[3] Constant goes

[1] Edward W. Constant, *The Origins of the Turbojet Revolution*. No. 5. (Johns Hopkins University Press, 1980), 68.
[2] Ibid., 69.
[3] Ibid., 72.

on to explain that, "The turbojet revolution is thought to represent a preeminent example of a presumptive-anomaly-induced radical technological change."[4]

Other examples of presumptive anomalies could include what Kaku describes as evolutions in technology advancement equaling a technological paradigm shift or a change in the fundamental way of conducting business. Kaku describes current, near-future and far-future technologies that will reshape the way the military fights.

The presumptive anomalies presented by Kaku include harnessing the power of magnets, the wind (including solar wind), advancements in computers, and artificial intelligence in robots.[5] Consider the computing power and size of computers in 1980 as compared to 2015. The anomaly is a computer that used to require an entire room now fits inside a watch and is exponentially more powerful. It is assumed that the computing power of the human brain will eventually be surpassed by the computing power of machines opening the door to artificial intelligence and artificial reasoning.

Sometimes requirement generation occurs through user observation or during mission execution. These requirements are not presumed or iterative; identifying them may improve integration, fill gaps in capabilities, or allow for greater interoperability among players. Existing in the culture of the U.S. military is a natural drive to innovate and progress.

Military Derived Requirements

Solutions to gaps in interoperability or integration of systems in complex systems oftentimes generate requirements. In 1991, during Operation Desert Storm, the U.S.

[4] Ibid., 73.
[5] Michio Kaku. *Physics of the Future: How Science Will Shape Human Destiny and our Daily Lives by the Year 2100*, (Anchor, 2012), 125.

military recognized a problem detecting large movements of men and machines across the deserts of Iraq. The development of the ground-moving-target-indicator (GMTI) radar system, and the ability to place this system on aircraft drastically changed the speed of information and the accuracy of maneuver forces to counter enemy advances in and around Kuwait. The Joint Surveillance Attack Radar System (JSTARS) was rapidly developed and fielded to satisfy this requirement. When "paired with extended-range attack systems-such as helicopters, Army tactical missile system (ATACMS) and joint assets-JSTARS enables commanders to rapidly locate and destroy targets at great depth."[6]

Just 15 years later, with greater technological advancements and more efficient aircraft the JSTARS is under the United States Air Forces recapitalization plan with a desire to field the next evolution of JSTARS in FY23.[7] Sometimes systems become so outdated that the integration of new technology requires patches and upgrades to ensure the system is still able to meet mission requirements. The military industrial complex of major military technology producers, and some up-and-coming smaller business, often push solutions to perceived or actual problems before the military identifies that a problem even exits.

Industry Driven Requirements

Tradeshows, technology symposiums, and industry days allow major United States and international industry partners opportunities to showcase solutions to issues

[6] Quincy R. Jones, "JSTARS' FSO/Aviation Officer Crewmembers." *Field Artillery* no. 1: 25, (January 1997), http://search.proquest.com.nduezproxy.idm.oclc.org/docview/231135087?accountid=12686. (accessed August 18, 2015)
[7] James Drew, "Revised JSTARS Plan Mitigates Risk and Extends Competition", *InsideDefense.Com's Aircraft Alert*, (June 2015), http://search.proquest.com.nduezproxy.idm.oclc.org/docview/1655693968?accountid=12686. (accessed August 18, 2015)

that the DoD may not even realize exist. In cases surrounding the development of fifth-generation fighter aircraft like the F-22 and the newest F-35, industry is driving solutions that were not part of the original design requirements. The Joint Strike Fighter (JSF) program is the largest acquisition program in U.S. history, DOD anticipated the development of 2,457 aircraft across all service branches and international orders.[8] The program did not start that way. In its humble beginnings in 1983, the JSF program was a forward looking presumptive anomaly that the service life of Air Force A-10 and F-16 fighter aircraft would expire and the development of a replacement aircraft was required. When the designs were being developed, program requirements for the United States Navy and Marine Corps were added to the development, then international requirements from Australia, the United Kingdom, and Canada crept in making the original program not only un-executable but over budget and over timeline.

John McCain, Senator from Arizona and Chairman of the Senate Armed Services Committee, expressed concern that Congress was being included in the military-industrial complex. Senator McCain stated, "I would like to focus on how the military-industrial-congressional complex has kept even some of the most poorly-performing programs funded…siphoning-off precious resources even while they go over-budget, face years of schedule delays and fail to deliver promised capability to the warfighter."[9]

McCain went on to share, "the military-industrial-congressional complex does not cause programs to fail. But, it does help create poorly-conceived programs…programs

[8] Monique M. Maldonado, "Qualitative Case Study on F-35 Fighter Production Delays Affecting National Security Guidance." (Walden University Press, 2015). 4. In ProQuest Dissertations & Theses Global, http://search.proquest.com.nduezproxy.idm.oclc.org/docview/1686804186?accountid=12686. (accessed September 12, 2015)

[9] Lanham, *Remarks by Senator John McCain on the "Military-Industrial-Congressional" Complex*, (Federal Information & News Dispatch, Inc., 2012), http://search.proquest.com.nduezproxy.idm.oclc.org/docview/911229117?accountid=12686. (accessed September 12, 2015)

that are so fundamentally unsound that they are doomed to be poorly executed."[10] This relationship between congressmen, industry, and the military is laden with tension as competing interests begin to drive requirements and programmatics. In the case of the F-35, 48 of the 50 states in the United States have a stake in the production of components of the aircraft. Industry driven requirements are not always in the best interest of the military due to fiscal constraints and the competing interests of the producer to make money and the military requirement to reduce spending.

This chapter described the three types of requirements generation that initiate the Technological Culture Model and drive reconsideration of a problem and potential solutions through innovation. The art of innovation is not unique to America, every society on earth exercises it to some level. Understandably, when the U.S. develops new technologies to satisfy requirements generated by gaps in capability or presumptive anomalies, the adversaries of the U.S. are conversely developing strategies to counter the new technology.

SECTION 2: *Technology Development*

The innovation and development of technological solutions to military requirements occurs in classified locations and under misleading monikers like Lockheed Martin's Skunk Works, or the Boeing Corporation's LabNet network of laboratories around the world. The DoD participates in technology development through offices like Checkmate and the various service research labs. "Most people …think of technology in terms of its product…as things or machines, observing with concern that the machines of

[10] Ibid., 3.

our culture often appear out of human control, threatening to trap and enslave, rather than to liberate."[11]

Technology development is more than just widgets; it is the entire enterprise of thought that may produce a tangible product. Richard Buchanan describes technology in terms of design theory and innovation. In the U.S., Silicon Valley is synonymous with cutting-edge design, leading technology, and the heart of industrial innovation. Large corporations like Boeing, Lockheed Martin, and Northrup Grumman compete for funding to develop technology and systems for the military and commercial enterprises alike. All technology producers, DoD and private industry, are bound not only by their creativity, but by budgetary constraints and oversight.

Budgetary Considerations and Strategic Direction

Each of the four uniformed services within the DoD has its own research and development (R&D) department. The Air Force has the Air Force Research Laboratory in Ohio, the Army has the Army Research Laboratory in Maryland, the Navy has their Navy Research Laboratory in Washington D.C., and the Marine Corps Warfighting Lab is in Virginia. Together these laboratories execute a considerable budget of $153.9 billion.[12] $90.4 billion is for procurement of new systems, $63.5 billion is dedicated to major defense acquisition programs where $11.3 billion is earmarked specifically for research, development, test and evaluation (RDT&E).[13] The DoD budget accounts for

[11] Richard Buchanan, "Wicked Problems in Design Thinking." *Design issues* (1992): 5-21.
[12] U.S. Department of Defense, Office of Management and Budget: *Program Acquisition Cost by Weapons System*, (Washington DC: Government Printing Office, 2015). http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2015/fy2015_Weapons.pdf (accessed September 12, 2015)
[13] Executive Office of the President of the United States: *The 2015 Budget: Science, Technology, and Innovation for Opportunity and Growth*; (Washington D.C.: Government Printing Office, March 2014). https://www.whitehouse.gov/sites/default/files/microsites/ostp/Fy%202015%20R&D.pdf (accessed 22 September 2015)

approximately 12.8% of the $3.9 trillion executable budget of the United States in FY15 while RDT&E accounts for just over .28% of the national budget.

Driving innovation are not only presumptive anomalies, but the NSS, the National Military Strategy (NMS), and the Quadrennial Defense Review (QDR). The NSS forecasts technological development and RDT&E. In 2015, President Barak Obama stated, "We [the United States] continue to set the pace for science, technology, and innovation in the global economy."[14] "Set[ting] the pace" does not happen without leading the world in RDT&E. In the State of the Union address in January 2016, President Obama declared, "nobody even comes close" to the technical capabilities of the United States.[15]

Military Research and Development

For years, the determination to bring R&D under DoD control was considered "in the best interest of national security."[16] Bringing R&D in house allows the technology to be governed, controlled, and funded through DoD budgets. Bringing R&D in-house was a concern to industry, which in turn drove private companies to develop their own R&D divisions, leading to innovative technologies that the DoD had not even considered. Today there are national and private R&D facilities around the world that spend billions of dollars researching solutions to problems in industry, society, and the military. The combination of military and private R&D allows flexibility and broadens the field of experts, which in turn facilitates creativity in design and problem solving. Due to

[14] U.S. President, National Security Strategy (Washington DC: Government Printing Office, February 2015), 2.
[15] U.S. President, *State of the Union Address*, (2016) https://www.whitehouse.gov/the-press-office/2016/01/12/remarks-president-barack-obama-%E2%80%93-prepared-delivery-state-union-address (accessed January 28, 2016)
[16] U.S. Congress, Office of Technology Assessment, *Defense Conversion: Redirecting R&D.* (Office Washington DC: Government Printing Office, 1993).

regulations and constrained budgets, the integration of government R&D facilities, personnel, and resources with the private sector is not always achievable.

Industry Research and Design

Never underestimate the impact of industry driven research and design. Private industry, usually at the company's own expense and research, brought the U.S. military projects like the SR-71 supersonic, high flying spy platform, and the F-117A, the first stealth fighter/bomber into Air Force inventory.[17]

Lockheed Martin Corporation's Advanced Programs Office, called "Skunk Works", developed the F-117A completely of its own accord, and expense, to highlight the design and production capabilities of the company and to showcase the idea of radar diffusing technology. Never did they anticipate that it would become one of the most amazing aircraft to ever fly on behalf of the U.S. military.

Another example of individual company innovation was the development of the "Tactical Display Framework" (TDF) by the Solipsys Corporation. TDF brought an innovative way to display and synthesize numerous RADAR sources into one comprehensive picture allowing battle managers and commanders to make decisions on asset prioritization, airspace deconfliction, and aircraft identification. Solipsys created TDF without the military coming to the company with a requirement to solve a problem. The company saw the problem and developed a solution to sell to the military on their own.[18] The two examples above illustrate how allowing companies to innovate and

[17] Ben R. Rich and Leo Janos. *Skunk Works: A Personal Memoir of my Years at Lockheed*. (Little, Brown, 2013), 68-87.

[18] The author attended a Trade Show at Nellis Air Force Base in the fall of 2004 where TDF was originally pitched to the USAF Weapons School for controlling aircraft on the Nevada Test and Training Range. Once purchased, TDF was implemented across the range and eventually purchased by USCENTCOM for use in their area of responsibility for command and control of air operations in Iraq and Afghanistan.

compete for military acquisition can sometimes solve technology gaps before they become critical requirements.

Bridging the Technology Gap between DoD and Industry

"With the passage of the Stevenson-Wydler Act of 1980, Congress established technology transfer as a legitimate mission of every Federal laboratory and has since encouraged DoD labs to enter into cooperative R&D programs with industry."[19] With the Bayh-Dole Act of 1980, Government Owned Government Operated (GOGO) labs, including the DoD labs, were given authority to grant private companies exclusive licenses to patents.

The Federal Technology Transfer Act (FTTA) of 1986 expanded these powers by allowing each federal agency to grant directors of GOGO labs the authority to enter into cooperative R&D agreements (CRADAs) with commercial partners and to negotiate licensing agreements. Sharing information between DoD research labs and commercial entities opens the door to reducing stovepipe driven gaps in interoperability, vulnerability, and integration.

Additional to the CRADA, "technology transfer legislation allows the DoD labs to contribute facilities, time, and personnel (but not funding) to R&D programs conducted jointly with industry. Industry may contribute facilities, personnel, and funding."[20] This cost reduction is an incentive to utilizing the legislation to the maximum extent, especially as budgets dwindle and oversight increases. Sharing labs and personnel helps to diffuse the cost of research and design between the company and the payroll

[19] U.S. Congress, Office of Technology Assessment, *Defense Conversion: Redirecting R&D.* (Office Washington DC: Government Printing Office, 1993). 12.
[20] Ibid., 14.

employees of the DoD; however, further legislation is required to continue closing the remaining intellectual and creative thinking gaps.

SECTION 3: *Acquisition of New Technology*

Acquiring new technology carries with it a tail of maintenance, sustainability, training, and integration costs. The acquisition process associated with purchasing new technology is very detailed and somewhat cumbersome. Despite the fact that this paper will not go into granular detail on the acquisition process itself, it is beneficial to have a basic understanding of the Joint Capabilities Integration and Development System (JCIDS). This system is designed to programmatically ensure technologies are adequately designed and tested to withstand the rigors of the military environment while ensuring that they ultimately satisfy the originally stated requirement.

Acquisition Process Overview

"Problems in major defense acquisition programs, when accurately identified, can be a source of guidance for improving acquisition management procedures."[21] The acquisition process in the DoD is not broken; however, it is cumbersome and complicated. At one time there was a Technology Development Strategy required by each program to detail 17 lines of effort for the program, including the acquisition approach, interoperability summary, and risk analysis. (Appendix 2)

In the latest DoD Instruction 5000.02 the Acquisition Strategy has replaced the Technology Development Strategy. The new streamlined Acquisition Strategy has 12

[21] Robert V. Johnson and John Birkler. *Three Programs and Ten Criteria Evaluating and Improving Acquisition Program Management and Oversight Processes Within the Department of Defense*. No. /MR-758-OSD. (RAND Corp Santa Monica, CA., 1996), 3.

areas of focus that are more generic and less defined than the previous development strategy. (Appendix 3) This updated approach to acquisition program management has diluted the requirements for the purchase and integration of emerging technology under the guise of making the process more efficient.

The acquisition process highlights the steps for technology development to fill requirements and estimates the timelines for purchase, testing, fielding, and ultimately disposition of government acquired technologies. Understanding the development cycle is informative to the model because the timelines are different for each set of technology development. An advanced tank will have a much longer acquisition timeline than a sophisticated truck.

Technology has three types of vulnerabilities: intrinsic, internal, and external. Understanding how these elements of vulnerability interact with a complex system is informative to the Technological Culture Model reminding that technology may cost more than just money.

Understanding Intrinsic Vulnerability

Intrinsic properties consist of the materials that make up an object, but that depends entirely upon what the object is like in itself. [22] Defined another way, "[a] thing has its intrinsic properties in virtue of the way that thing itself, and nothing else is."[23] Like many of the definitions in this thesis, theorists differ on bounding the differences between and intrinsic property and an internal one. An intrinsic property is a property that is internal to an object, or a technology, that is uniquely related to only that technology. Take for example the properties of human behavior. Intrinsic human

[22] Robert Francescotti, "How to Define Intrinsic Properties." *Noûs* (1999): 590-609.
[23] D. Lewis, "Extrinsic Properties", *Philosophical Studies* (1983): 197-200.

properties include a person's genetic disposition, personality, neural networks, and fingerprints. These are properties that are unique to every individual on the planet.

In technology, every item shares some properties but each has its own intrinsic property. Take a flashlight, there are thousands of types of flashlights in the marketplace, but none of them are exactly the same. They all emit light, they all have some type of switching mechanism to turn them on or off, and something powers them. Despite all of these similarities, how they emit the light, how they are switched on and off, and how they are powered may all be different. Intrinsically the flashlights are similar but not the same. 'Proprietary' technology is a business way of identifying intrinsic technological properties used in the development or implementation of a product.[24] This distinction is important when discussing acquisition because proprietary technology may be more expensive and potentially less interoperable within the complex system and has the potential to drive the generation of new requirements.

Identifying Internal / External Vulnerabilities

Internal vulnerabilities are components in a system or technologies that are vulnerable to breaking, wearing out, or not operating such that the technology performs its functions error-free. Think of an automobile, there are many internal components of the engine that could fail because of the intrinsic vulnerability of the manufactured materials, the internal vulnerabilities that exist because of the violent interaction between the components and the risk to component breakdown or destruction.

External vulnerabilities are those that expose weakness to the system or technology that allows external factors to degrade or negate the system. Reference the

[24] Joel West, "How Open is Open Enough? Melding Proprietary and Open Source Platform Strategies." *Research policy* 32.7 (2003): 1259-1285.

automobile example above, external vulnerabilities are the exposed parts of the engine, the wires that are susceptible to moisture or hungry animals, the metal that is susceptible to rust and the environment, or somebody taking a hammer to the pulleys and engine parts causing the system to fail. Every piece of technology has internal and external vulnerabilities. Understanding what those vulnerabilities are and deducing the level of risk the vulnerabilities create is of utmost importance to the understanding of why an overly technology dependent military may be at odds with national security.

U.S. reliance on satellite systems is a great example of increasing risk by accepting intrinsic, internal, and external vulnerabilities. The U.S. and her allies have become reliant on satellite communication that allows individuals in the U.S. to communicate directly with pilots flying missions in the Middle East. While the use of this technology appears to reduce the kill chain timeline, enhance command and control, and provide near real time oversight of military operations to the President and his cabinet of advisors anytime they desire, the fact remains that while the U.S. becomes more and more dependent on satellite systems, adversaries constantly seek ways to diminish, degrade, or destroy this capability in defense of their interests.

Intrinsic vulnerabilities abound in the chemicals, materials, and requirements for satellite systems to remain in orbit, operate properly, and maintain contact with their handlers on earth. Additionally, internally all of the pieces and parts must operate in perfect harmony ensuring robust two-way communication while initiating commands remotely.

Externally, outer space is an extremely inhospitable operating environment where electrically charged dust, electromagnetic clouds, solar magnetic pulses, and radiation are

just a few of the elements that can affect satellite operations. Satellites are vulnerable to being hacked, digital or mechanical electronic attack, and to destruction by the growing amount of space debris orbiting the earth. The requirement for constant and consistent communication will be a mainstay for the U.S. military and her allies well into the future, thus, the need to protect space assets by reducing their vulnerabilities is imperative.

Preparing for this reality, "the needs of tactical military communications have given rise to the development of small road and air transportable terminals which can be quickly shifted to a new location and deployed within a short time under field conditions to provide secure and reliable communication between moving units." [25] Chatterjee goes on to say,

> In order to meet the demands of command and control of highly mobile units/moving platforms such as the ships and aircraft with modest bandwidth requirements, satellite systems built around lower frequencies (UHF) evolved to fill the critical need of tactical communications. UHF systems, utilizing smaller antennas with wider beam widths, do not require high accuracy beam pointing mechanisms and can easily be accommodated on mobile platforms. Although, UHF terminals can be made small and relatively inexpensive, the available bandwidth and the degree of protection from interfering sources is limited.[26]

Acknowledging that there are vulnerabilities in the system is not the same as acknowledging that there is an increased risk in the system. Over reliance on satellite capabilities is clouding the perceived risk of use by increasing the demand signal to communicate across the world. Identifying the internal and external vulnerabilities of a piece of technology and further identifying how the integration of the technology into a

[25] C. K. Chatterjee, "Present and Future Trends in Military Satellite Communication Systems." *Defense Science Journal* 43.1 (2013): 37-42.
[26] Ibid., 45.

complex operational military system potentially makes the system more vulnerable is more difficult than it sounds.

Consider the introduction of self-driving cars on national highways and city streets: does the risk to other human-operated vehicles increase or decrease? Technology experts tell us that the risk decreases because technology can make more rapid, safer decisions than a human being. But, intuitively people want to be in control of their actions, including driving vehicles and a self-driving vehicle perceptually means relinquishing some of that control. Professor Nass, a sociology professor at Stanford University, explained that societal comfort with technology is gained through experience, and acceptance occurs when people have seen a technology work enough times collectively. He also pointed out that it took a long time for people to develop trust in air transportation, something that is taken for granted today.[27]

Over time, it is natural to become accepting of technologies that make life simpler, allow further reach, and promise greater safety. None of these conclusions account for the threat over-technologizing the world poses for nations states, governments, or militaries. Most of the time, it is when technology is initially introduced that its vulnerabilities and shortcomings emerge, its effect on other systems, and the extent of its usefulness. The next section will introduce considerations in fielding new technology and its effect on complex systems like that of the military.

SECTION 4: *Fielding New Technology*

After acquiring new technology, it must be tested, evaluated, and fielded. System vulnerability is compounded by the previously described intrinsic, internal, and external

[27] Clifford Nass and Youngme Moon. "Machines and Mindlessness: Social Responses to Computers." *Journal of Social Issues* 56. (2000), 243.

vulnerabilities inherent in every piece of technology. Once integrated, the technology becomes a new component of the overall system which then assumes the sum of the individual vulnerabilities of all the components together. In military terms, the level of acceptable risk is based on component vulnerability factors within the system. As the acceptable level of risk (ALR) increases, the acceptance of potential system failure also increases.

Understanding the Complexity of the System

To understand the complexity of the military as a system of systems, consider first how the components of a campaign, namely Air, Land, Sea, Marine, and Special Operations, work in symphony in every engagement across a battlespace. In the Air Component, the Air Tasking Order (ATO) generation cycle alone is a complex orchestra of hundreds of leaders, planners, platforms, and systems working together to generate, prioritize, and deliver air power for a single 24-hour period.

Knowing that "a plan never survives first contact with the enemy"[28] it is important to understand that the executors of any plan must be adaptable and the technology used to execute that plan must be gracefully degradable. Graceful degradation is the ability to fall back on other systems when the primary, secondary and tertiary systems begin to fail.

For example, when you cannot use a phone, use email; if email does not work, send a text message; if the cell towers are out, send a fax; if the phone lines are down, write a letter and mail it. Each iteration of a graceful degradation plan has a cost of time,

[28] Michael S. DuPerier, *The Bush National Security Strategy: What's All the Fuss About*. No. AU/AF Fellows, 2004. Air Force Fellows Program, (Air University Press, Maxwell AFB, AL., 2004).

resources, and sometimes clarity. Degraded operations can add unanticipated complexity to any system and any campaign.

In a complex system, any change introduced to the system results in greater complexity and can potentially generate new requirements. Systems approach chaos when tenets like adaptability, graceful degradation, or stability are not achievable. When new technology is introduced into a military operating environment, oftentimes there are "growing pains" associated with the integration. It is not difficult to understand that each aircraft in the Air Force has unique capabilities and specific tactics for employment including communication standards, data transfer standards, and flight characteristics. In the USAF inventory today are over fifty different aircraft. If even ten of them operate in the same environment at the same time, the complexity in airborne tactics alone is immense. Quadruple that when all four services are flying their aircraft in the same operating environment. The complexity in an operational environment is easy to visualize but difficult to simplify.

Integration Considerations

When integrating new technology into a system, the effects are readily apparent. Systems, like human beings, are adverse to change, especially once they have reached a comfortable stability. Consider the integration of Unmanned Aerial Vehicles (UAV) in military operations. At first, the satellite requirements were overwhelming. The ability to integrate the slow moving, latently responsive, and less than maneuverable aircraft into the airspace required rethinking and retooling of airspace structures and requirements. Today, fighting without the capabilities of Remotely Piloted Aircraft (RPA) is untenable.

The risk to life of the pilot of the UAV is near zero; however, the risk to other manned aircraft operating in proximity to an unmanned vehicle has increased.

The system initially rejected the integration of unmanned aircraft by moving them far away from the battles, employing them where no other aircraft were flying, and complaining about their lack of responsiveness to changing directions. In Iraq in 2005 MQ-1 Predator drones were gaining popularity among ground force commanders. Introducing an increasing number of unmanned aircraft into a saturated manned airspace was not only difficult, but was sometimes dangerous. Drones are susceptible to losing the connection to their handlers and when that happens the drones assume a pre-programmed flight profile, sometimes flying through congested airspaces with no warning and no ability to change their course. Adapting to this possibility required greater restrictions on airspace and altitude assignments of manned aircraft constraining an already difficult operating environment.

There is no such thing as 'seamless' integration when introducing new technology into complex but stable systems. Like any environment, there will always be perturbations when introducing change. Time is a key factor in returning any system to stasis. Despite leadership desires to make it quick, there is no predictably established timeline. Sometimes it will take minutes, other times it may take days for a system to return to equilibrium. The recipe for success is in the test and evaluation (T&E) phase of technology development. It is in the T&E phase that integration is a focus and the new technology is put through the paces with other components of a system. Integrating new technology is the first step in identifying second and third order effects on the system.

Interoperability Considerations

Interoperability can be difficult to achieve without cooperation with the many manufacturers of the components of a piece of technology. For example, Boeing Corporation will not share proprietary information with Northrop Grumman Corporation because of the perceived power of keeping certain trade secrets. That is not to pick on the Boeing Corporation; Northrop Grumman would be equally unwilling to share proprietary data. Because of this corporate bureaucracy, achieving interoperability of systems is difficult. Expand that idea to include the international community of manufacturers. History has shown that warfighting usually includes a coalition of allies. Aircraft, sea craft, and communication equipment do not always interoperate without patches, release-ability allowances, and upgrades. This creates friction on the battlefield just as it does in the corporate environment.

A focus on interoperability early in the developmental cycle will minimize component vulnerability in the system. The side effect of this is the potential to become reliant on one single piece of technology to meet all actors' needs, creating a potential single point of failure or massive external vulnerability to the system. The balance between sharing information, technology, and equipment is crucial to successful operations.

Corporations have attempted to solve this problem by purchasing smaller, more specialized companies to keep production "in-house" versus sharing information with a competitor. The monopolization of American business is a factor in the production, cost, and interoperability challenges the military faces. Every now and again a piece of technology comes along that changes the character of warfare. These changes have many

terms including disruptive technologies, revolutions in military affairs, and paradigm shifts. Being familiar with revolutions in technology shapes technology reliance and fuels the perpetual nature of the Technological Culture Model.

SECTION 5: The Role of Disruptive Technology

Revolutions in Military Affairs

Over the centuries, thinking about warfare has changed due to the development and employment of RMA or "disruptive"[29] technologies on the battle space. In the Technological Culture Model, disruptive technologies are ones that reset the cycle. They can be introduced during any point in technology development and are only limited by creativity and imagination. Disruptive technologies are revolutionary and have an impact at every level of warfare. These technological advances in warfare often change the very character of warfare and disrupt the perpetual cycle of evolutions in technology.

Technological Advances in Warfare

Three specific RMAs have influenced changes in the character of warfare. First, the invention of gunpowder and the revolution of gunpowder weaponry; second, the aircraft revolution in World War 1 (WWI) and 2 (WWII) resulting in the establishment of a separate U.S. military service; and finally, the development, use, and proliferation of nuclear weapons. Each RMA adjusted the consideration of variables like time, distance, terrain, and scale.

Disruptive technology is important to the Technological Culture Model because it acts like a reset button. Introducing disruptive technology into a system changes the

[29] Andrew Oram, *Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology*. (O'Reilly Media, Inc., 2001), 14.

character of that system. As described above, RMAs change the character of warfare and because they change the character, they introduce opportunity for greater innovation, counter-technology development, strategy, and new tactical employment considerations. These changes drive the perpetual nature of the model renewing a cycle of technology dependence in the military. Disruptive technology does not mean that it is disruptive in design or nature. It means that the employment or integration of such technology redefines the environment, may require reframing technologies in the acquisition pipeline, or may negate capabilities as a whole. For example, aircraft technology absolutely changed the thinking and practice of warfare and the U.S. military never looked back. Once airpower integrated with ground and surface operations the very character of war changed. The process of integrating airpower reset the technological culture model inspiring new innovations and the initiation of new acquisition programs, thus a disruptive technology and an RMA.

CHAPTER 3: BREAKING THE CYCLE

If having a technological culture has made the United States military technology dependent, can it break the cycle? When is it appropriate to keep the system as is and to what extent is the nation inadvertently accepting vulnerability? Answers to these questions are nebulous because there is no U.S. strategy guiding technology research and development. To understand how and when to break the cycle it is useful to look at the Joint Strike Fighter (JSF) program, its production nuances, and its extended fielding timeline due to what Senator McCain termed the "military-industry-congressional complex."[1] Inserting politics into the model not only made it more complex, it also increased the amount of vulnerability in the program.

Seeking Joint Solutions

Logically, combining requirements across the joint community leads to the development of technology that fulfils the requirements for more than one service. Doing this would solve interoperability issues and allow the immediate integration of technology into the joint environment. Unfortunately, the JSF rejects this notion because since becoming a joint project, the implementation timeline has been delayed, requirements have significantly increased, and the per-unit cost soared causing some allies like Canada to cancel their order completely. Logically, joint solutions should reduce spending and make the services and coalition partners more interoperable.

The truth is, because of individual service requirements, congressional constituent corporate influence, and proprietary technologies, fielding timelines and budgets are

[1] Lanham, *Remarks by Senator John McCain on the "Military-Industrial-Congressional" Complex*, (Federal Information & News Dispatch, Inc., 2012), http://search.proquest.com.nduezproxy.idm.oclc.org/docview/911229117?accountid=12686. (accessed September 12, 2015)

merely guesses. With the rapidity of technological changes, the acquisition process simply cannot keep pace with technology development; meaning, by the time the military introduces new technology, it is already outdated, and in some extreme cases, obsolete. If a truly joint solution is attainable, the next step is to reduce the idea-to-fielding timeline so that technology is not immediately obsolete right after fielding.

Reducing the Idea-to-Fielding Timeline

The final argument to break the cycle is reducing the idea or requirement to fielding timeline. The development of Project Liberty (MC-12W) program went from requirement to fielding in one year at a significant cost reduction to other systems.[2] Compared to the 23 years the JSF has been in production, the MC-12W is a good case study in rapid technology fielding to meet joint needs on the battlespace. Marco Iansiti's writing on the framework for managing the space between the creation and the application of technology is informative to integrating new technologies in the operational environment.[3] Reducing the idea-production-fielding timeline will reduce the vulnerability of technology obsolescence and keeps the most current instruments in the hands of the operator versus in the lab.[4]

What should this timeline look like? According to Gordon Moore, a founder of the Intel Corporation, "computer power doubles about every eighteen months."[5] Using this framework, if the technology timeline from idea to fielding takes longer than eighteen

[2] Steven J. Tittel, "Liberty and Lethality: Integrating MC-12W Liberty and Light Attack/Armed Reconnaissance Aircraft Operations." *Monograph*, (School of Advanced Military Studies, Command and Gerneral Staff College, Leavenworth, KS., 2010), 4.
[3] Iansiti Marco, *Technology Integration: Making Critical Choices in a Dynamic World*. (Harvard Business Press, 1998), 42.
[4] Michio Kaku. *Physics of the Future: How Science will Shape Human Destiny and our Daily Lives by the Year 2100*. (Anchor, 2012), 124.
[5] Ibid., 127.

months, it is likely the computer power originally used in the technology will have doubled, creating a technology gap that will grow over time. In the case of the JSF, during the 23 years of work on the project, computer processing capabilities had doubled nearly fifteen times. When the first JSF experiences combat, the technology inside will be years behind the computing power of the 21st century.

The future is not all bleak. In the acquisition process, spiral upgrades are built into the plan so that systems and capabilities can be updated on a routine basis based on technology and requirement changes over the lifecycle of the product. In the example of aircraft technology, every so-many hours (different for each platform), the planes are sent into depot for overhauls and maintenance updates prior to beginning their next spiral period. This allows the platforms to maintain the "best" technology for their function and helps to close the gap that exists between fielded systems and changing technology.

CONCLUSION

The nineteenth century philosopher John Stewart Mill once said, “The source of everything respectable in man either as an intellectual or as a moral being is that his errors are corrigible…the whole strength and value of human judgment, depends on the one property, that it can be set right when it is wrong.”[1] Once an issue associated with technological culture and technology dependence has been raised, it becomes a moral obligation to seek corrective actions to reduce dependence and vulnerability. This is easier said than done. Technology is so woven in U.S. culture that the idea of living without it is unthinkable. Understanding the vulnerabilities within technologies and acknowledging dependence on using it is the first step in correcting the trend and recognizing where technology dependence has become a strategic risk.

Because the U.S. is a technological culture, the U.S. military has become technology dependent. This dependence has made the military more vulnerable and has plunged the DoD into a perpetual cycle of purchasing technology to fill shortfalls resulting from reductions in manpower, technology evolutions, and to "maintain the leading edge." Because technology is increasing in per-unit cost, the DoD purchases fewer items, increasing the impact of minimal losses in combat. Reversing this trend requires better integration, complementary technologies among the services, and decreasing the innovation to fielding timeline.

Understanding the perpetual nature of the Technological Culture Model, it is easy to ascertain that culture, experiences, and backgrounds critically contribute to technology

[1] Richard J. Arneson, "The Enforcement of Morals Revisited." *Criminal Law & Philosophy 7*, no. 3 (October 2013): 435-454. http://link.springer.com/article/10.1007/s11572-013-9240-y#/page-1 (accessed December 29, 2015).

dependence. This dependence, if not recognized, can increase vulnerability and risk at the strategic level, operational level, and tactical levels of war.

There are common misperceptions that using technology is less expensive to maintain than manpower and that technology can fill the gaps created when militaries downsize force strength. Removing human capital from the force structure of the military equates to huge monetary cost savings, as the service is no longer responsible for annual pay, insurance, healthcare, equipment, training, and sustainment. It is not uncommon for the military to turn to technology to increase system efficiencies so those remaining can absorb the responsibilities of those who are now gone.

While technology can assist in streamlining some operations, the support requirements to keep the technology up to date, to solve issues when the technology malfunctions, and to allow graceful degradation to occur actually increases manpower and cost requirements. Logically, with fewer people and more automation, when the automation malfunctions, is degraded, or completely fails there is a greater impact on the system than there would have been if one person were to have gotten ill or left. The overall system is less flexible and adaptable to changing situations.

The misperception is the idea that the DoD can control the cost of these support systems and technologies by setting fiscal boundaries on support contracts. Contracting support has its own set of limitations and issues. When contracting for a fixed amount of time, contractors are not always willing to complete a job early or stay late to ensure every detail is completed because there is job assurance in going slower, only working the specified contracted time, taking every possible break, and exploiting every possible loophole in the contract. Holding contractors accountable takes time and energy away from

military members' ability to focus on other tasks and further exacerbates the loss of military manpower.

A second fallacy is that the military with the best technology will win. Technology also increases tactical, operational, and strategic vulnerability because of the increased potential for hack, exploitation, denial, or degradation. The U.S. military has been engaged in fighting in the Middle East for over a decade. In Afghanistan, during the early phases of the war, adversary military members were able to hack into unsecure drone feeds, gaining information on strike planning, targets, and the location of operations. This allowed the intelligence community the opportunity to warn key individuals. ultimately extending the fighting in certain regions of Afghanistan.[2]

In Iraq and Syria, the Islamic State of Iraq and Syria (ISIS) has been able to use internet social media to extend their reach and share their message with sympathizers worldwide. Using terror tactics, this organization has been able to exploit vulnerabilities in identification technology, passport replication technology, and open border surveillance allowing them freedom of maneuver throughout Europe. Technology has yet to be the critical element in decisive victory. Looking back, many believe that the atomic bombs dropped on Hiroshima and Nagasaki ended WWII. The truth is the Japanese were already on the verge of collapse. While atomic technology was devastating, it was not the only reason the Japanese surrendered.[3] Technology does have a role in warfare; however, it is not a panacea for victory.

[2] Noah Shachtman, "Insurgents Intercept Drone Video in King Size Security Breach." *Wired.*, (December 2009).
[3] Herbert Feis, *The atomic bomb and the end of World War II*. (Princeton University Press, 2015). 62.

In the absence of perfect technology, vulnerability and risk are areas the U.S. military must manage every day. Understanding that technology is only one of many tools used in solving the nation's most difficult problems and taking into account the increase in vulnerability by fielding new technologies into the operational schema is important. Being dependent on anything increases risk and creates critical vulnerabilities exploitable by adversaries. There is a converging point where the consistent acceptance of vulnerabilities becomes "normalized" and its practice becomes so commonplace that the thought of fighting, engaging, or executing without technology seems unthinkable. This convergence point is the place where technology dependence begins.

Approximately every ten years, the U.S. military incorporates a new generation of technology dependent recruits. Based on the inflow and outflow of military members through retirement, separation, and discharge approximately every 30 years, the integration and incorporation of technology in daily operations becomes understandably commonplace. There will be military members each year who have no idea that the military operated without a certain piece of technology because it is all they have known in their military experience. Over time, a paradigm associated with advanced technology forms and the vulnerability associated with the technology becomes unconsciously accepted, re-baselining the starting place for risk analysis.

Fifty years ago, a soldier, sailor, marine, or airman would not have even considered using an airborne network to collaborate near real-time on the battlefield. Beyond line of sight radios were in the High Frequency spectrum, were unencrypted, and were difficult to understand based on a propagation of up to 4000 miles. Today, satellites allow for beyond line of sight communications, airborne networks pump data to decision

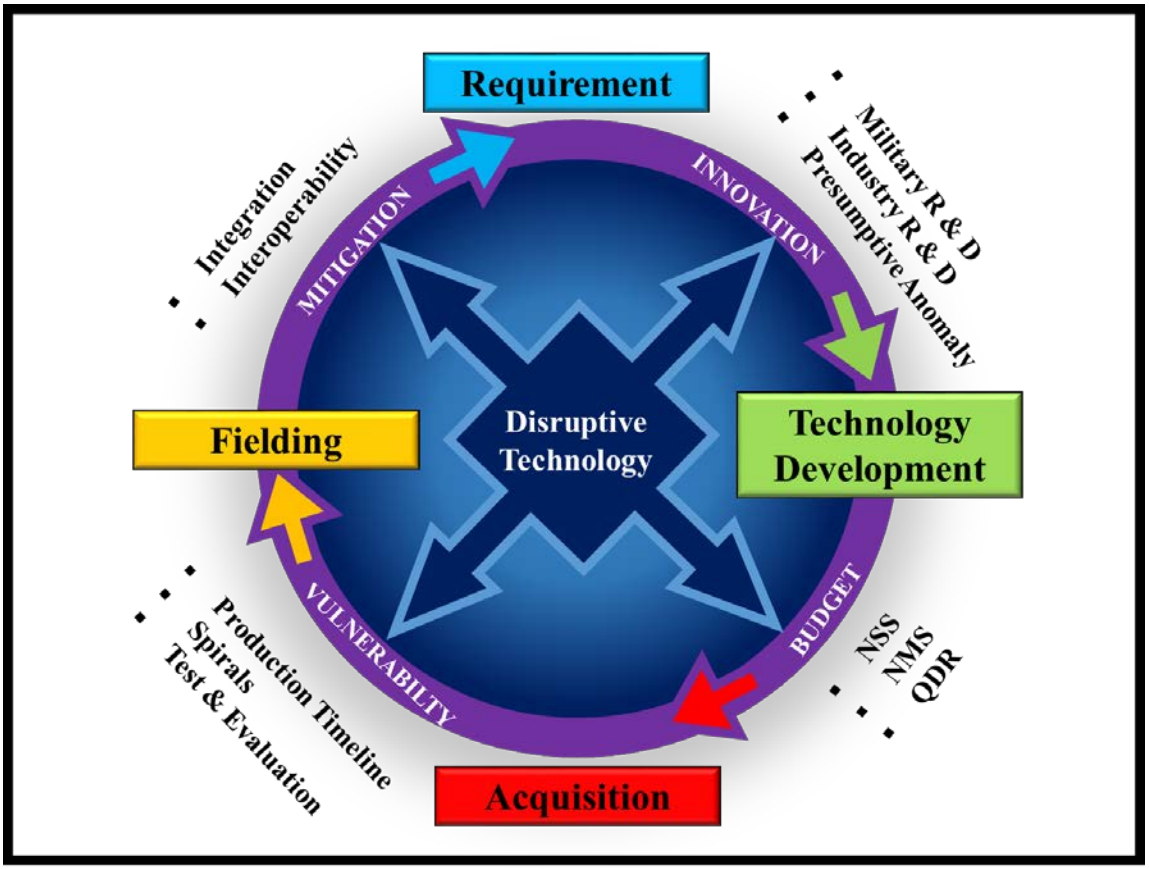
makers for maximum battlefield awareness, and drones extend the visual reach of commanders thousands of miles. Employing these technologies makes the U.S. and her allies more lethal, more efficient, and more effective. Their use also makes the U.S. and her allies more vulnerable to hack, attack, and setback.

The uses of these and other technologies have become common practice. Today's paradigm of technology enabled lethality, speed, and range is amazing; however, it is important to recognize that the risks are also increasing. Strategy is not without risk. The 2015 NSS recognizes that technology will be among U.S. interests now and into the future. It is incumbent on the DoD to recognize that technology dependence increases vulnerabilities from the tactical to the strategic level. The U.S. military will continue to be the best military in the world so long as it cautiously and deliberately integrates technology into operations, acknowledges where technological vulnerabilities create risks, and continues to seek collaborative, interoperable, and joint solutions to capability gaps.

It is time to identify where technology has driven unanimously accepted risks before it is too late. Determining where the U.S. military is technology dependent is not difficult. A good starting place is in information system technology and communications. Conducting exercises that reduce the use and availability of collaborative systems like computers, phones, the internet, and some beyond line of sight radios will highlight areas where the military can gracefully degrade and still meet mission requirements with ingenuity and creativity. It is time to reduce technology dependence in the U.S. military through recognition, risk analysis, and practice.

APPENDIX 1

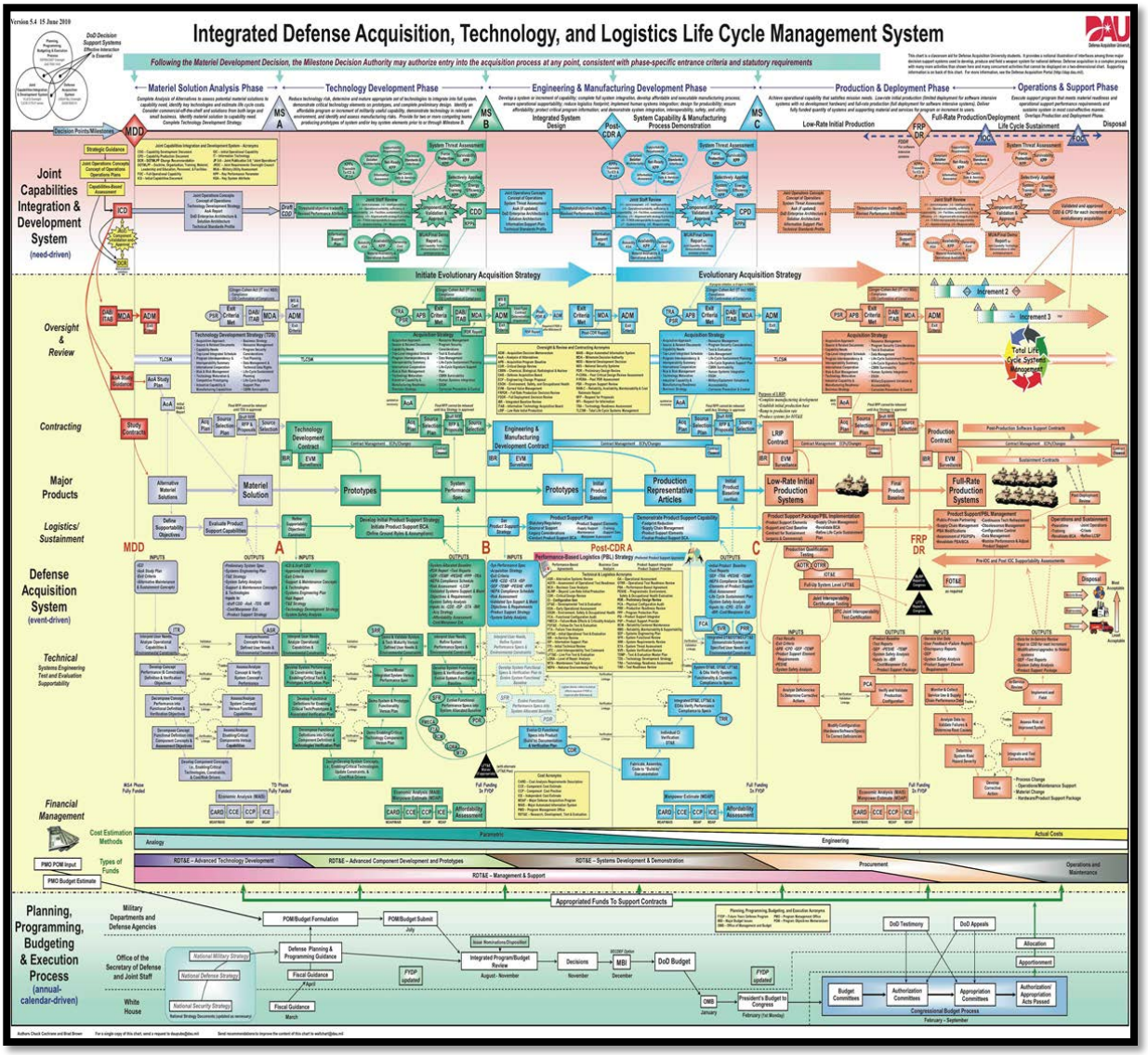
THE TECHNOLOGICAL CULTURE MODEL



Using this model shows how a technological culture can lead to technology dependence when solutions to requirements are actual technologies and not changes in integration, implementation, or organization. Technological culture develops when iterations of the above cycle result in a lifestyle where non-technical solutions are ignored in lieu of seeking solutions involving new technologies.

APPENDIX 2

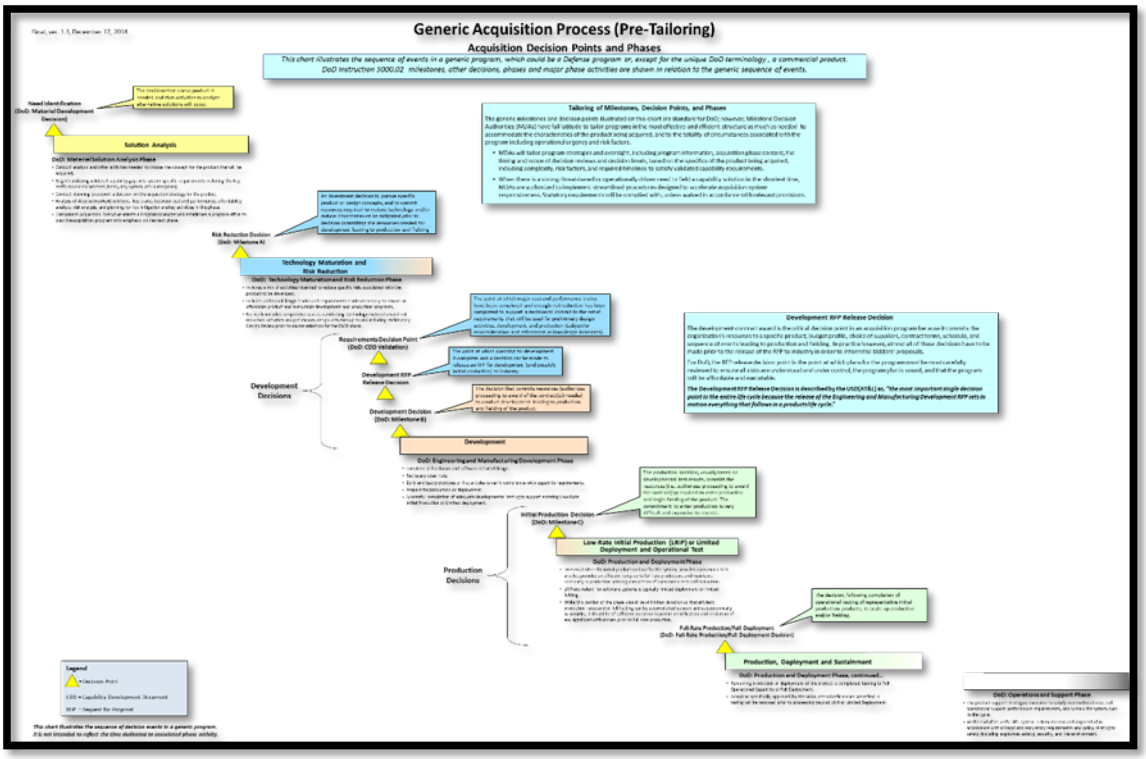
JOINT, INTEGRATED DEFENSE ACQUISITION, TECHNOLOGY and LOGISTICS LIFE CYCLE MANAGEMENT SYSTEM[1]



[1] This shows the Joint Capabilities Integration and Development System (JCIDS) process http://www.public.navy.mil/spawar/PEOC4I/ASPG/Documents/APSG_Manuals/files/Integrated_Def_Acq_Management_Frmwk.pdf (accessed October 12, 2015)

APPENDIX 3

THE NEWEST (2015) GENERIC ACQUISITION PROCESS (Pre-Tailorying) [1]



[1] This shows the updated Joint Capabilities Integration and Development System (JCIDS) process as of 2014. https://dap.dau.mil/aphome/Documents/Defense%20Acquisition%20Waterfall%20Chart%20with%20color%20enhancements%2017%20Dec%20final%20(3).pdf (accessed October 12, 2015).

BIBLIOGRAPHY

Books

Bijker, Wiebe Eco. *Vulnerability in Technological Cultures*. Maastricht University, 2009.

Caforio, Giuseppe. *Handbook of the Sociology of the Military*. Springer Science & Business Media, 2006.

Chatterjee, C. K. "Present and Future Trends in Military Satellite Communication Systems." *Defense Science Journal* 43.1, 2013.

Constant, Edward W. *The Origins of the Turbojet Revolution*. No. 5. Johns Hopkins University Press, 1980.

Douglas, Jack D. *The Technological Threat*. Prentice-Hall, 1971.

Feis, Herbert. *The Atomic Bomb and the End of World War II*. Princeton University Press, 2015.

Finlan, Alastair. *Contemporary Military Culture and Strategic Studies: US and UK armed forces in the 21st Century*. Routledge, 2013.

Kaku, Michio. *Physics of the Future: How Science Will Shape Human Destiny and Our Daily Lives by the Year 2100*. Anchor, 2012.

Mahnken, Thomas G. *Technology and the American way of war*. Columbia University Press, 2008.

Marco, Iansiti. *Technology Integration: Making Critical Choices in a Dynamic World*. Harvard Business Press, 1998.

Marquis, Samuel S. *Henry Ford: An Interpretation*. Wayne State University Press, 1923.

Morris, Ian. *War! What is it Good For?: Conflict and the Progress of Civilization from Primates to Robots*. Macmillan, 2014.

Rich, Ben R., and Leo Janos. *Skunk works: A Personal Memoir of my Years at Lockheed*. Little, Brown, 2013.

Thompson, Clive. *Smarter Than You Think: How Technology is Changing Our Minds for the Better*. Penguin, 2013.

Articles

Arneson, Richard J., "The Enforcement of Morals Revisited." *Criminal Law & Philosophy 7*, no. 3 (October 2013), http://link.springer.com/article/10.1007/s11572-013-9240-y#/page-1 (accessed December 29, 2015).

Axelrod, Norman N., "Embracing Technology: The Application of Complexity Theory to Business." *Strategy & Leadership*, no. 6 (October 1999), http://search.proquest.com.nduezproxy.idm.oclc.org/docview/194363285?accountid=12686. (accessed October 5, 2015).

Callaway, S. K., & Hamilton, R. D. "Exploring Disruptive Technology: The Structure and Control of Internal Corporate Ventures", *International Journal of Organizational Analysis, 14*(2), (October 2006), http://search.proquest.com.nduezproxy.idm.oclc.org/docview/198743036?accountid=12686 (accessed 22 November 2015)

Drew, James. "Revised JSTARS Plan Mitigates Risk and Extends Competition", *InsideDefense.Com's Aircraft Alert*, (June 2015), http://search.proquest.com.nduezproxy.idm.oclc.org/docview/1655693968?accountid=12686. (accessed August 18, 2015)

DuPerier, Michael S. *The Bush National Security Strategy: What's All the Fuss About*. No. AU/AF Fellows 2004. Air Force Fellows Program, Air University Press, Maxwell AFB, AL., 2004

Estes, Adam Clark. "Your Phone's Battery Use Lets Spies Track Your Movements", *Gizmodo*, 20 Feb 2015, http://gizmodo.com/spies-can-track-you-through-your-phones-battery-use-eve-1686978418 (accessed January 20, 2016)

Francescotti, Robert. "How to Define Intrinsic Properties." *Noûs*, 1999.

Freidersdorf, Conner, "Obama Supporters Know his Drone War is Indefensible", *The Atlantic: Politics*, Jun 2012, http://www.theatlantic.com/politics/archive/2012/06/obama-supporters-know-his-drone-war-is-indefensible/258218/ (accessed January 15, 2016)

Hardy, Cynthia, and Steve McGuire, "Organizing Risk, Discourse, Power, and 'Riskification'" *Academy of Management Review* 41., no. 1: 80-108, (January 2016) (accessed 21 January 2016)

Johnston, Alastair Iain. "Thinking About Strategic Culture." *International security*, 1995.

Jones, Quincy R. "JSTARS' FSO/Aviation Officer Crewmembers", *Field Artillery* no. 1: 25, (January 1997), http://search.proquest.com.nduezproxy.idm.oclc.org/docview/231135087? (accessed August 18, 2015).

Knepper, Jennifer. "Nuclear Weapons and Iranian Strategic Culture." *Comparative Strategy* 27.5, 2008.

Lewis, D., "Extrinsic Properties", *Philosophical Studies*, 1983.

Loayza, Norman, and Claudio E. Raddatz. "The structural determinants of external vulnerability." *World Bank Policy Research Working Paper* 4089, 2006.

Lutzenhiser, Loren. "Social structure, culture, and technology: Modeling the driving forces of household energy consumption." *Research directions*, 1997.

Majumdar, Dave, "Did Iran Just Create a Stealth Drone from Captured American Tech?", *The National Interest*, November 24, 2014., http://nationalinterest.org/feature/did-iran-just-create-stealth-drone-captured-american-tech-11683 (accessed December 15, 2015).

Maldonado, Monique M. 2015. "Qualitative Case Study on F-35 Fighter Production Delays Affecting National Security Guidance" *Walden University Press*, 2015. In ProQuest Dissertations & Theses Global, http://search.proquest.com.nduezproxy.idm.oclc.org/docview/1686804186?accountid=12686. (accessed September 12, 2015).

Nass, Clifford, and Youngme Moon. "Machines and Mindlessness: Social Responses to Computers." *Journal of Social Issues. ,*2000.

Oram, Andrew. *Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology*. O'Reilly Media, Inc., 2001.

Shachtman, Noah. "Insurgents Intercept Drone Video in King Size Security Breach." *Wired.*, December 2009.

Slack, Jennifer Daryl, and J. Macgregor Wise. "Culture and Technology." *A Primer, New* 2005.

Snell, J., "Chaos Theory and Post Modernism", *Education, 130*(2), (February 2009). http://search.proquest.com.nduezproxy.idm.oclc.org/docview/196414440?accountid=12686 (accessed 27 September 2015).

Wallis, S. E., "The Complexity of Complexity Theory: An Innovative Analysis", *Emergence: Complexity and Organization*, 11(4), (April 2009). http://search.proquest.com.nduezproxy.idm.oclc.org/docview/214151202?accountid=12686 (accessed 15 December 2015).

West, Joel. "How Open is Open Enough? Melding Proprietary and Open Source Platform Strategies." *Research policy* 32.7, 2003.

Woodbury, Robert S.. "The Legend of Eli Whitney and Interchangeable Parts". *Technology and Culture* 1.3, 1960.

DoD Publications

United States Department of Defense. Office of the Chairman of the Joint Chiefs of Staff. *National Military Strategy*. Washington, D.C.: U.S. Government Printing Office. June 2015.

_____. *JP 3-0, Joint Operations*. Washington, D.C.: U.S. Government Printing Office. 11 August 2011

_____. Office of the Secretary of Defense. *National Defense Strategy*. Washington, D.C., 2015.

_____. Office of the Secretary of Defense. *Quadrennial Defense Review Report*. Washington, D.C., 4 March 2014.

Documents, Reports, Statements, Studies

Executive Office of the President of the United States: *The 2015 Budget: Science, Technology, and Innovation for Opportunity and Growth*; Washington D.C.: Government Printing Office, March 2014. https://www.whitehouse.gov/sites/default/files/microsites/ostp/Fy%202015%20R&D.pdf (accessed 22 September 2015)

U.S. President, *National Security Strategy.* Washington DC: Government Printing Office, February 2015.

U.S. President, *State of the Union Address*, Washington DC: Government Printing Office, January 2016. https://www.whitehouse.gov/the-press-office/2016/01/12/remarks-president-barack-obama-%E2%80%93-prepared-delivery-state-union-address (accessed January 28, 2016)

Lanham, "Remarks By Senator John McCain on the 'Military-Industrial-Congressional' Complex", *Federal Information & News Dispatch, Inc.* 2011, http://search.proquest.com.nduezproxy.idm.oclc.org/docview/911229117?accountid=12686. (accessed 12 September 2015)

Johnson, Robert V., and John Birkler. *Three Programs and Ten Criteria Evaluating and Improving Acquisition Program Management and Oversight Processes Within the Department of Defense*. No. MR-758-OSD, RAND Corp Santa Monica, CA., 1996.

Tittel, Steven J. "Liberty and Lethality: Integrating MC-12W Liberty and Light Attack/Armed Reconnaissance Aircraft Operations." *Monograph*, School of Advanced Military Studies, Command and General Staff College, Leavenworth, KS., 2010.

United States Congress. Office of Technology Assessment. *Defense Conversion: Redirecting R&D.*" Washington D.C.: U.S. Government Printing Office, 1993. (accessed 14 September 2015)

United States Department of Defense. Office of the Chairman of the Joint Chiefs of Staff. *The National Military Strategy of the United States of America, 2015: The United States Military Contribution to National Security*. Washington, D.C.: Government Printing Office, 2015.

_____. Office of Management and Budget. Program Acquisition Cost by Weapons System, Washington D.C.: U.S. Government Printing Office, 2015, http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2015/fy2015_Weapons.pdf. (accessed 12 September 2015)

Wise, Macgregor J. "Technological Culture: A Presentation to the Asia Cultural Forum 2006." *Kwangju, Korea* (June 2006). http://www.cct.gov.kr/data/acf2006/mobile/mobile_keynote2_Macgregor.pdf. (accessed August 15, 2015)

Internet Sources

Boot, Max. Testimony before the House Armed Services Subcommittee on Terrorism, Unconventional Threats, and Capabilities, 29 June 2006. http://www.cfr.org/publication/11027/ (accessed November 20, 2015).

Boyd, John. *"OODA Loop."* http://www.nwlink.com/~donclark/leadership/ooda.html (accessed November 14, 2015)

CJCS Risk Analyis brief, https://dde.carlisle.army.mil/LLL/DSC/ppt/L14_CRA.pdf, 2004 (accessed November 12, 2015)

http://acqnotes.com/acqnote/acquisitions/technology-development-strategy (accessed September 20, 2015)

http://acqnotes.com/acqnote/careerfields/acquisition-strategypm (accessed September 20, 2015)

https://dap.dau.mil/aphome/Documents/Defense%20Acquisition%20Waterfall%20Chart%20with%20color%20enhancements%2017%20Dec%20final%20(3).pdf (accessed October 12, 2015)

http://www.public.navy.mil/spawar/PEOC4I/ASPG/Documents/APSG_Manuals/files/Integrated_Def_Acq_Management_Frmwk.pdf (accessed October 12, 2015)

VITA

Lieutenant Colonel Keven P. Coyle commissioned in 1998 through the Reserve Officer Training Corps at the University of Utah. He completed Air Battle Manager training graduating with the Commandants Trophy as the top graduate for his class in fall 1999. A few years later, he became an instructor at the USAF Weapons School serving as Flight Commander, Assistant Operations Officer and then Director of Staff for the Weapons School Commandant. Following service at the Weapons School, Lieutenant Colonel Coyle attended the US Army Command and General Staff College, graduating in June 2010. After completed the Army's course, he became the Chief of Intelligence, Surveillance, Reconnaissance, and Current Operations for Joint Special Operations Command Aviation Tactics Evaluation Group. Prior to attending the Joint Advanced Warfighting School, Lieutenant Colonel Coyle served as the Commander of the 960th Airborne Air Control Squadron, Tinker Air Force Base, Oklahoma where he executed national policy supporting the National Command Authority through rapid world-wide employment of the E-3 Airborne Warning and Control System. He directly supervised 340 United States and Canadian Forces and the operation of six E-3 aircraft valued at over $1.8 billion. Lieutenant Colonel Coyle is a Master Air Battle Manager with more than 1,500 hours in the E-3, including over 350 combat and combat support hours. He has flown in numerous contingency operations including Operations NORTHERN WATCH, NOBLE EAGLE, ENDURING FREEDOM, IRAQI FREEDOM, and has multiple deployments in support of counter-terrorist operations worldwide. Lieutenant Colonel Coyle has a Master of Science degree from the University of Oklahoma.